

EFFICIENT ROUTING PROTOCOL TO DETECT AND PREVENT SYBIL ATTACK IN WIRELESS SENSOR NETWORK

PRAMEET KAUR¹ & SANDEEP SINGH KANG²

¹Department of Computer Science & Engineering, CGC, Landran, Mohali, Punjab, India

²HOD, Department of Computer Science & Engineering, CGC, Landran, Mohali, Punjab, India

ABSTRACT

Wireless sensor network (WSN) is a constantly growing technological platform with extremely large and novel applications. WSN's are being used in many applications such as habitat monitoring (to observe wildlife), health monitoring, logistics (equip goods with sensor nodes), military purposes, and home automation. WSN are prone to various security attacks one of which is Sybil attack, in which one node takes multiple identities and misbehaves in the network. In this paper, we propose a security based on LEACH routing protocol against Sybil attack. LEACH (Low Energy Adaptive Hierarchy) routing protocol is the conventional clustering communication protocol which is commonly used in Wireless Sensor Networks. Major issue with LEACH routing protocol is energy consumption. In order to balance the energy consumption of each node, the nodes are selected as cluster head randomly and circularly. The mechanism is set up to detect Sybil attack based on the distance and hop count between the nodes and the prevention is done using encryption technique which is based on unique identities of the nodes. Three performance parameters: Throughputs, energy consumption, packet overhead are calculated. Their values show the efficiency of the proposed protocol.

KEYWORDS: Wireless Sensor Network, LEACH Protocol, Encryption, Sybil Attack

INTRODUCTION

WSN's (Wireless sensor Networks) are a latest type of networked systems, characterized by strictly limited computational and energy resources, and an ad hoc operational environment. The security of wireless sensor networks has been researched considerably over the past few years and which is a great issue. WSN have characteristics that are unique to them, such as the ability to withstand unfavorable environmental conditions, dynamic network topology, communication failures, large scale of deployment, scalable node capacity, node mobility, unattended operation as well as limited power, to name a few. WSN consist of base stations, which have more resources such as more energy that act as a gateway between the sensor nodes and the end user. The energy source of sensor nodes in wireless sensor networks (WSN) is usually powered by battery, which is not likely, even impossible to be recharged or replaced. Therefore, improving the energy efficiency and minimizing the message overhead are the major challenges in sensor networks.

WSNs are highly susceptible to routing attacks because of their dynamic topology and limited resources. The open nature of the wireless medium makes it easy for outsiders to listen to network traffic or interfere with it. These factors make these networks vulnerable to several different types of attacks. In most of the wireless attacks, an attacker can also easily eavesdrop on communication, record packets, and replay the packets and can also insert bogus (fake) packets. Sybil attacks can cause intense damage to the route discovery mechanism used in several routing protocols. In Sybil attack one node takes another node identity in a network and utilizes them in the same physical equipment which leads to loss or alter of data to make the network destroyed.

The assignment of routing protocol is to establish routing between sensor node and Sink node, and send reliable data. The original intention of LEACH is to resolve the energy exhausting about routing protocol in WSN. But with the wide application of LEACH Protocol, more attention to the security trouble in LEACH has been paid. This paper reviews the performance of energy aware Leach against Sybil attack and its prevention using encryption scheme following requisite functions for every terminal end.

LEACH ROUTING PROTOCOL

LEACH is a self-organizing, adaptable clustering protocol which uses equalized energy load distribution among the SNs in the WSN. The operation of LEACH is split into rounds and each round is divided into two phases namely as: setup and steady-state phase. Steady-state phase is always long compared to the set-up phase to minimize the overhead.

In LEACH protocol, the SNs arrange themselves into local clusters, with one node acting as the leader which defined as cluster head (CH) and rest of the nodes act as ordinary nodes which are remembers of the cluster head. To prolong the lifetime of the network, LEACH includes randomized rotation of the high-energy CH and performs local data fusion to transmit the amount of data being sent from the CHs to the BS. If BS is far away from the network then the energy of CHs will be affected as only CHs are directly communicating with the BS. Set of clusters will be different for different time interval and the decision to become a CH depends on the amount of energy left at the SN.

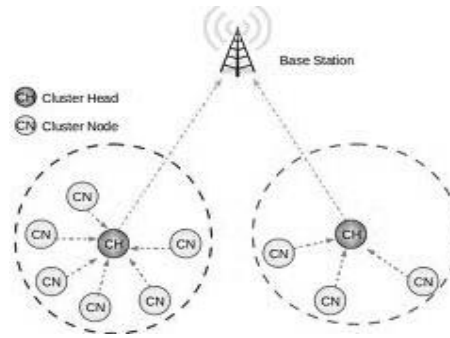


Figure 1: Network Model

Steps

The operation is divided into rounds, where the each round starts with a set-up phase, when the clusters are organized, followed by the steady-state phase. In order to minimize the load, the steady-state phase is long compared to set-up phase. The basic flow chart of the LEACH protocol is shown in the figure 2. It takes place in following step:

- Advertisement phase: Initially, each node decides whether or not to become a cluster-head for the current round. This decision is based on the number of times the node has been a cluster-head. The decision is made by selecting the node n choosing a random number between 0 and 1. If this is less than threshold $T(n)$, the node becomes cluster-head for the current round. The threshold level is set by:

$$T(n) = p / 1 - p * (r \bmod (1/p)) \text{ if } n \in G$$

$$= 0 \text{ otherwise}$$

Where the p = desired percentage of cluster heads

r = the current round

G is the set of the nodes that have not been cluster-heads in the last rounds.

- **Cluster Set-up Phase:** In this each node inform the cluster head that it will be a member of the cluster by transmitting energy.
- **Schedule Creation:** The cluster head receives all the messages as request to be a part of cluster. Cluster head creates a TDMA schedule to inform nodes that when it transmit data.
- **Data Transmission:** As the TDMA schedule is fixed data transmission begins. Aggregation of data takes place which is send to base station by cluster head. After this four steps are repeated.

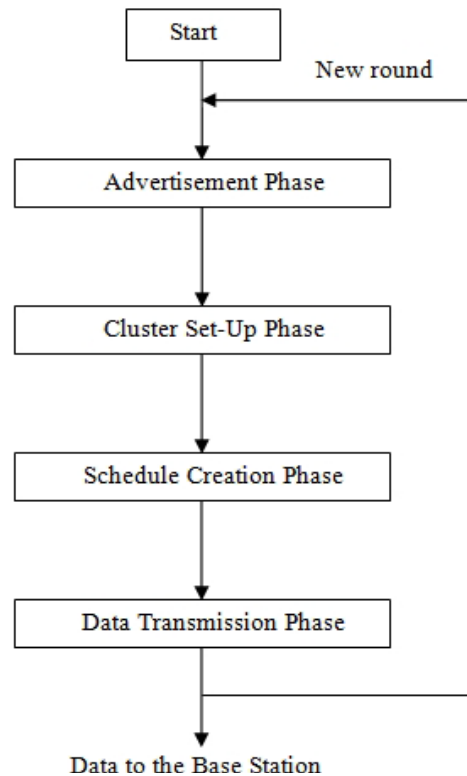


Figure 2: Processing of LEACH

SYBIL ATTACK

Sybil attack is referred to as a process in which malicious device illicitly taking on multiple identities. A malicious device's additional identities are referred to as Sybil nodes. In Sybil attack one node replicates another node's identity and utilizes them in same physical equipment and misbehaves. The Sybil attack taxonomy are developed in its different forms to better understand the implications. Several orthogonal attributes such as direct vs. indirect communication and fabricated vs. stolen identities are considered.

Attribute I: Direct vs. Indirect Communication

- **Direct Communication:** One way by which the Sybil attack can be carried out is for the Sybil nodes to communicate directly with the legitimate nodes of network. When a legal node sends a radio message to a Sybil node, one of the malicious devices listens to the message. Similarly, messages sent from Sybil nodes are in fact sent from one of the malicious devices.
- **Indirect Communication:** In this type of the attack, legitimate nodes are not able to communicate directly with the Sybil nodes rather than one or more of the malicious devices may claim to be able to reach the Sybil nodes. Messages sent to a Sybil node are routed via one of these malicious nodes, which constitute to pass on the

message to a Sybil node.

Attribute II: Fabricated vs. Stolen Identities

A Sybil node can take an identity in one of two ways. It can generate a new identity, or it can take an identity from a legitimate node.

- **Fabricated Identities:** In some cases, the attacker can simply generate random new Sybil identities. Suppose, if each node is identified by a 32-bit integer, the attacker can simply allocate each Sybil node a random 32-bit value.
- **Stolen Identities:** Given a method to establish the identity of legitimate node identities, an attacker cannot fabricate new identities. Suppose the name space is deliberately limited to prevent attackers from inserting new identities. In this case, the attacker requires assigning other legitimate identities to Sybil nodes. This stealing of identity may go undetected if the attacker destroys or temporarily disables the impersonated nodes.

PROPOSED SCHEME FOR SYBIL ATTACK DETECTION AND PREVENTION

In this, we will describe a method to detect and prevent Sybil attack. We start the procedure by adding security routing LEACH protocol on the wireless sensor network (WSN's). In this a group of mobile nodes are created. One of node is elected as base stations. Base station sends HELLO packets to all other nodes for topology verification. Nodes with minimum packet drops are chosen as trust nodes. The elected trust nodes now become the head nodes with a group of its own member nodes. The member nodes send their ID and power value to the head nodes. The head node checks for nodes with the power value less than threshold value. If the situation is true then those nodes are detected as Sybil nodes. The abnormal nodes are selected as receivers for next detection phase. In the next detection phase two nodes closer to Sybil nodes are selected as sender's s1 and s2. The two Sybil nodes are selected as receiver's r1 and r2. Packets are sent from s1 and s2 to both the receiver's. Since both the identities are present at the same node, there is collision of packets leading to packet drops. Sybil attack occurs if any one of the following condition takes place.

- The distance between the receivers is found. If the distance is zero, then the node suffers from Sybil attack.
- If nodes are very close, then the nodes will be detected as Sybil nodes even if they are not.

Encryption technique is applied to prevent Sybil attack on WSN's. It is done by distributing the unique identities to each node of the cluster. Then the routing procedure in the cluster is checked to verify if there was a hop between the Sybil identities. If there exists a hop between the Sybil identities, then the nodes are not Sybil nodes. If there is no hop, the nodes are confirmed to be under attack and they will be removed from the network. In the next phase two nodes closer to Sybil nodes are selected as sender's s1 and s2. The hop between the Sybil nodes and Sybil identities are analyzed. If the hop exists then the nodes are not Sybil nodes.

Both the detection and prevention scheme is implemented using all the requisite data as per simulation necessity and key which have to be implemented on basis of binomial distribution. The binomial distribution is the discrete probability distribution of the number of successes in a sequence of n independent yes/no experiments, each of which yields success with probability p . If the random variable X follows the binomial distribution with parameters n and p , we write $X \sim B(n, p)$. The probability of getting exactly k successes in n trials is given by the probability mass function:

$$f(k; n, p) = \Pr(X = k) = \binom{n}{k} p^k (1 - p)^{n-k} \text{ for } k = 0, 1, 2, \dots, n \text{ where}$$

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

is the binomial coefficient, hence the name of the distribution. The formula can be understood as follows: we want k successes (p^k) and $n - k$ failures $(1 - p)^{n-k}$.

Following Steps Takes Place

- In a network simulator we add a new routing protocol.
- Implementation of LEACH on WSN.
- Add energy to all the nodes of WSN which is deployed using LEACH.
- Implementation of Sybil attack in LEACH routing protocol of a network.
- Detection of Sybil attack using distance between nodes and hop count in the nodes.
- Prevention is proposed using an encryption technique.
- On the basis of this various parameters are proposed such as throughput, packet overhead and energy consumption.

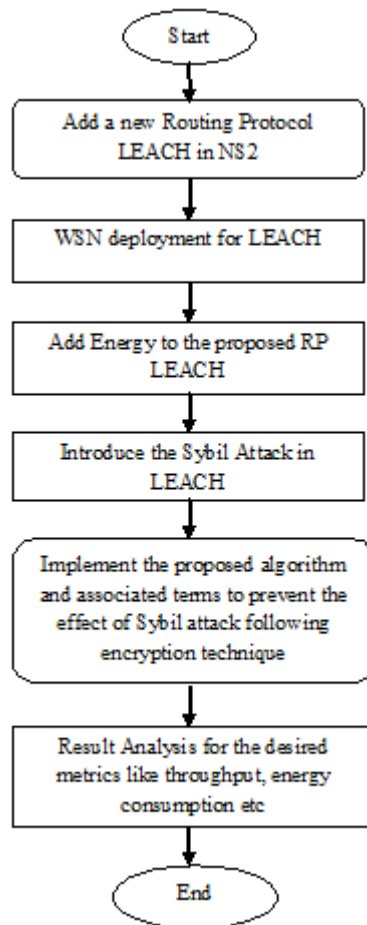


Figure 3: Flow Chart

SIMULATION AND PERFORMANCE ANALYSIS

We use NS-2 simulation to carry out simulation. NS-2 is an event-driven tool useful in studying the dynamic

nature of computer network. It provides the simulation of wired as well as wireless network functions and protocols (e.g., routing algorithms, TCP, UDP). In general, NS2 provides users with a way of specifying such network protocols and simulating their corresponding behaviours.

Table 1: Simulator Parameters

Parameter	Values
Simulator	NS-2
Simulation Duration	450 sec
Topology	2500 meter X 2500 meter
No. Of nodes	103
Maximum segment size	512
Traffic type	FTP (TCP)
Routing protocol	LEACH
Channel Type	Wireless Channel
Mobility Model	Two Ray Ground Propagation Model
Network Interface Type	Wireless PhyIEEE 802.11

RESULTS AND DISCUSSIONS

Throughput

Is the average rate of successful message delivery over a communication channel. The throughput is measured in kilo bits per second (kbps or kbit/s). The figure 4 shows the impact of Sybil attack on the WSN .The variation in the value is due to Sybil attack and sometimes reaches zero because of packet drop. Greater the value of throughput means better the performance of the protocol.

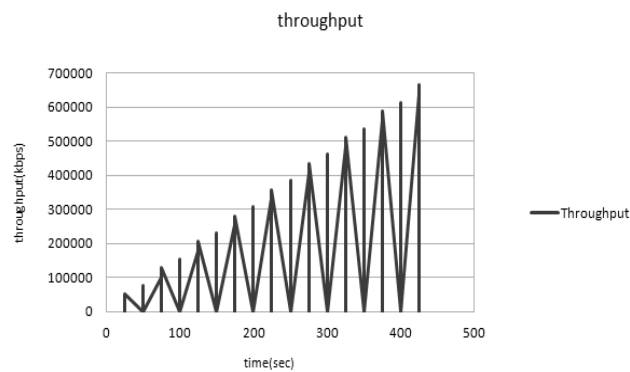


Figure 4: Impact of Sybil Attack on Network throughput

- **Packet Overhead:** is defined as number of packets dropped during transformation. Minimum the number of packet dropped better is the performance of the protocol.

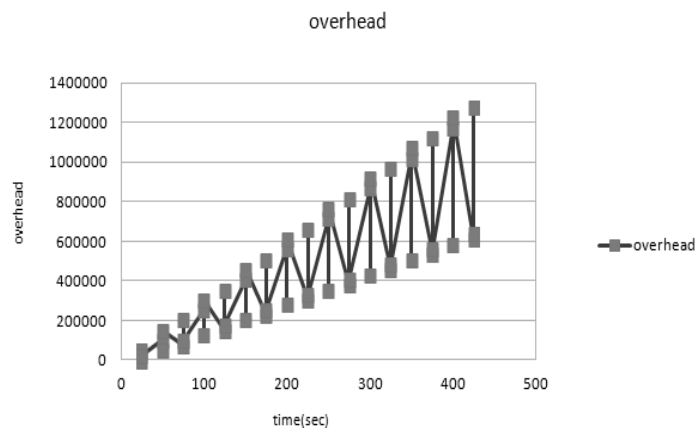


Figure 5: Impact of Sybil Attack on Network Overhead

Energy Consumption

Is defined as the consumption of energy or power. It is the amount of energy consumed during transfer of message from one node to another. The figure 6 shows the impact of Sybil attack on network energy consumption. Minimum the value of energy better is the performance of the protocol. It is measured in joules.

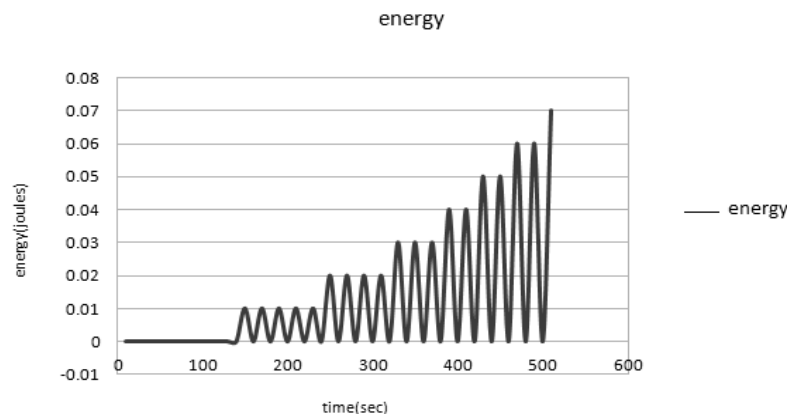


Figure 6: Impact of Sybil Attack on Network Energy

CONCLUSIONS

Nowadays, the Sybil attack is a major problem that suffers the wireless sensor network badly. In this paper, we focused over the detection and prevention in wireless sensor network. For this, we have proposed a robust and simple measure to detect Sybil attack. The proposed work clearly depicts the effect of detection using energy efficient LEACH routing protocol and its prevention using encryption scheme. The proposed work mainly works over the throughput, packet overhead and energy consumption. LEACH saves more energy, makes energy consumption distribute more evenly, and prolongs network's survival period. The simulation results are performed to reveal the performance of the proposed algorithm to detect and prevent approach.

REFERENCES

1. Jianyin, L., (2012) "Simulation of Improved Routing Protocols LEACH of Wireless Sensor Network" 7th International Conference on Computer Science & Education (ICCSE 2012) July 14-17, 2012. Melbourne, Australia (pp.662-666).
2. Tahir, H., Shah, S., (2008) "Wireless Sensor Networks – A Security Perspective" 12th IEEE International Multitopic Conference, December 23-24, (pp.189-193).
3. Lu, Y., Zhang, D., Chen, Y., Liu, X., and Zong, P., (2012) "Improvement of LEACH in Wireless Sensor based on Balanced Energy Strategy" IEEE International Conference on Information and Automation Shenyang, China, June (pp.111-115).
4. Jun, L., Hua, Q., Yan, L., "Modified LEACH algorithm In Wireless Sensor Network Based on NS2" 2012 International Conference on Computer Science and Information Processing (CSIP) (pp.604-606).
5. Xie, M., Han, S., Tian, B., Parvin, S., (2011) "Anomaly detection in wireless sensor networks: A survey" Journal of Network and Computer Applications 34 (pp.1302–1325).
6. Burgner, D., Wahsheh, L., (2011) "Security of Wireless Sensor Networks" Eighth International Conference on Information Technology: New Generations (pp.315-320).

7. Yanjing, S., Yanjun, H., Beibei Z., Xue, L., (2011) “An energy efficiency clustering routing protocol for WSNs in confined area”, *Sciencedirect Mining Science and Technology (China)* 21 (pp.845–850).
8. Wang, S., Yan, K., Wang, S., Liu, C., (2011) “An Integrated Intrusion Detection System for Cluster-based Wireless Sensor Networks”, *Science Direct Expert Systems with Applications* 38 (pp.15234–15243).
9. Patel, D., Patel, M., Patel, K., (2011) “Scalability Analysis in Wireless Sensor Network with LEACH Routing Protocol” *IEEE* (pp.123-128).